CTSC

CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

Practical Cybersecurity for Open Science Projects

The need for cybersecurity in science projects (at any scale) and first steps

Craig Jackson, Chief Policy Analyst, CACR and Co-PI, CTSC
Susan Sons, Senior Security Analyst, CACR and CTSC

Contributors:
Bob Cowles, CACR / CTSC / Brightlite Information Security
Von Welch, Director, CACR and PI, CTSC

Indiana University

27 April 2016

trustedci.org/trainingmaterials

Center for Trustworthy Scientific Cyberinfrastructure

The NSF Cybersecurity Center of Excellence

CTSC's mission is to provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

NCSA

PITTSBURGH SUPERCOMPUTING CENTER

THE UNIVERSITY of WISCONSIN MADISON

NSF

Outline

1. Introduction: Audience, Goals, Caveats, Terminology
2. Cybersecurity & Science
3. Cybersecurity Programs
4. Programmatic Must-Do's (at any size/complexity)

-1-
Introduction

The audience for today's session

CTSC's work spans the full range of NSF-funded projects and facilities.

Today, we're focused on smaller science projects...

- Unlikely to have dedicated security personnel or funding
- Unlikely to need tons of policy and process
- Relationships (e.g., with home institution) are particularly important
- But, can still be working with highly valuable, sensitive data and IT infrastructure.

Goals of this session

Provide you:

1. A sense of cybersecurity's relevance to science projects.
2. A sense of the complexity and scope of cybersecurity.
3. A sense of how cybersecurity programs can help you cope with that complexity (and protect your science).
4. A few "must-do" action items that are truly do-able and truly important.

And:

5. Get your questions on the table.

Caveats & Terminology

The views and conclusions contained herein are those of the author(s) and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the National Science Foundation or Indiana University.

Note on Terminology: We may use terms that have very specific meaning at IU; if so, we are using those terms generally and are *not* referring to IU's definitions.

e.g., "Sensitive data" - https://kb.iu.edu/d/augs

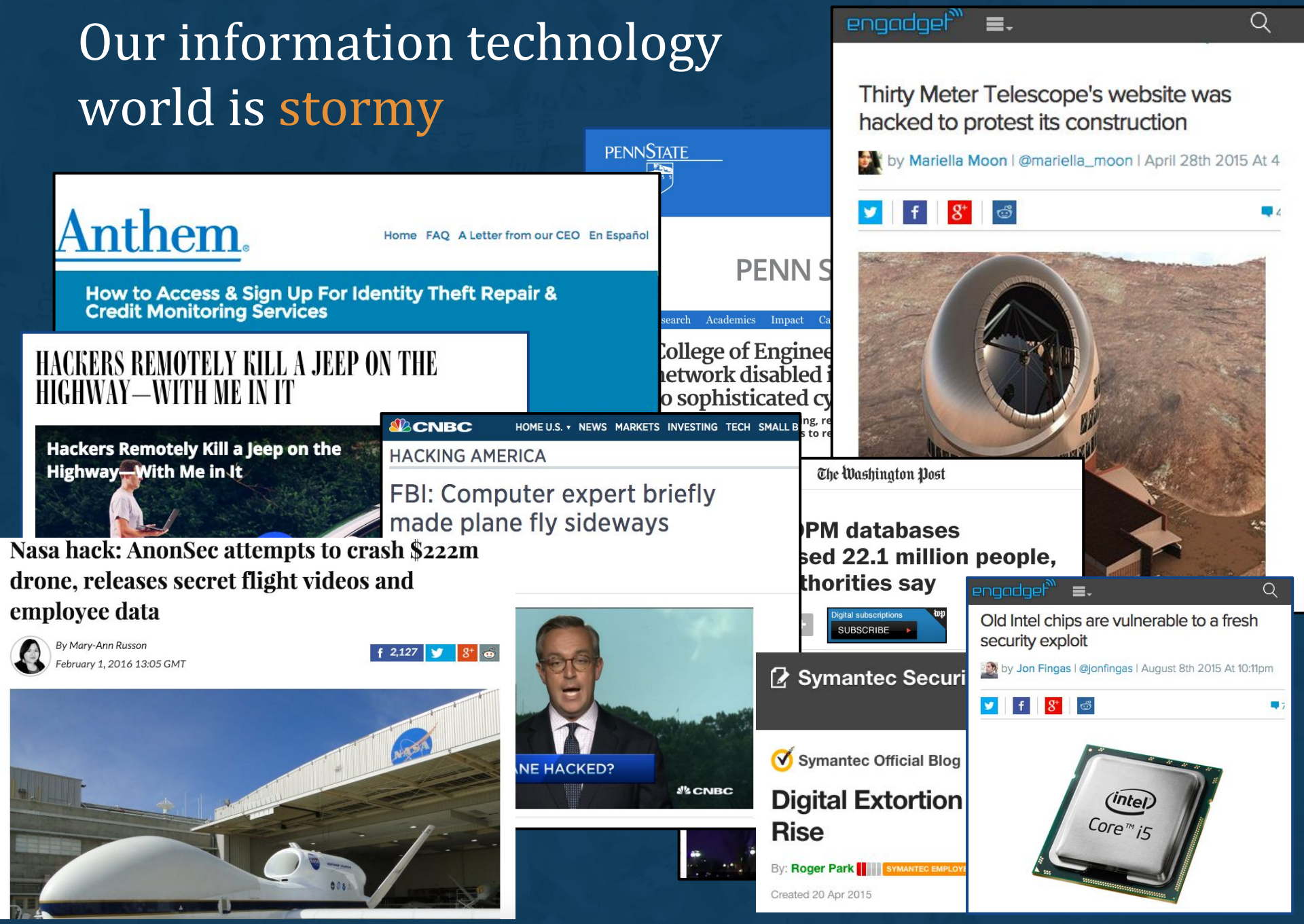
Some more notes about terminology

1. We use "information security" and "cybersecurity" more or less interchangeably. We often prefer the former, but have gotten trapped in the cybereverything.

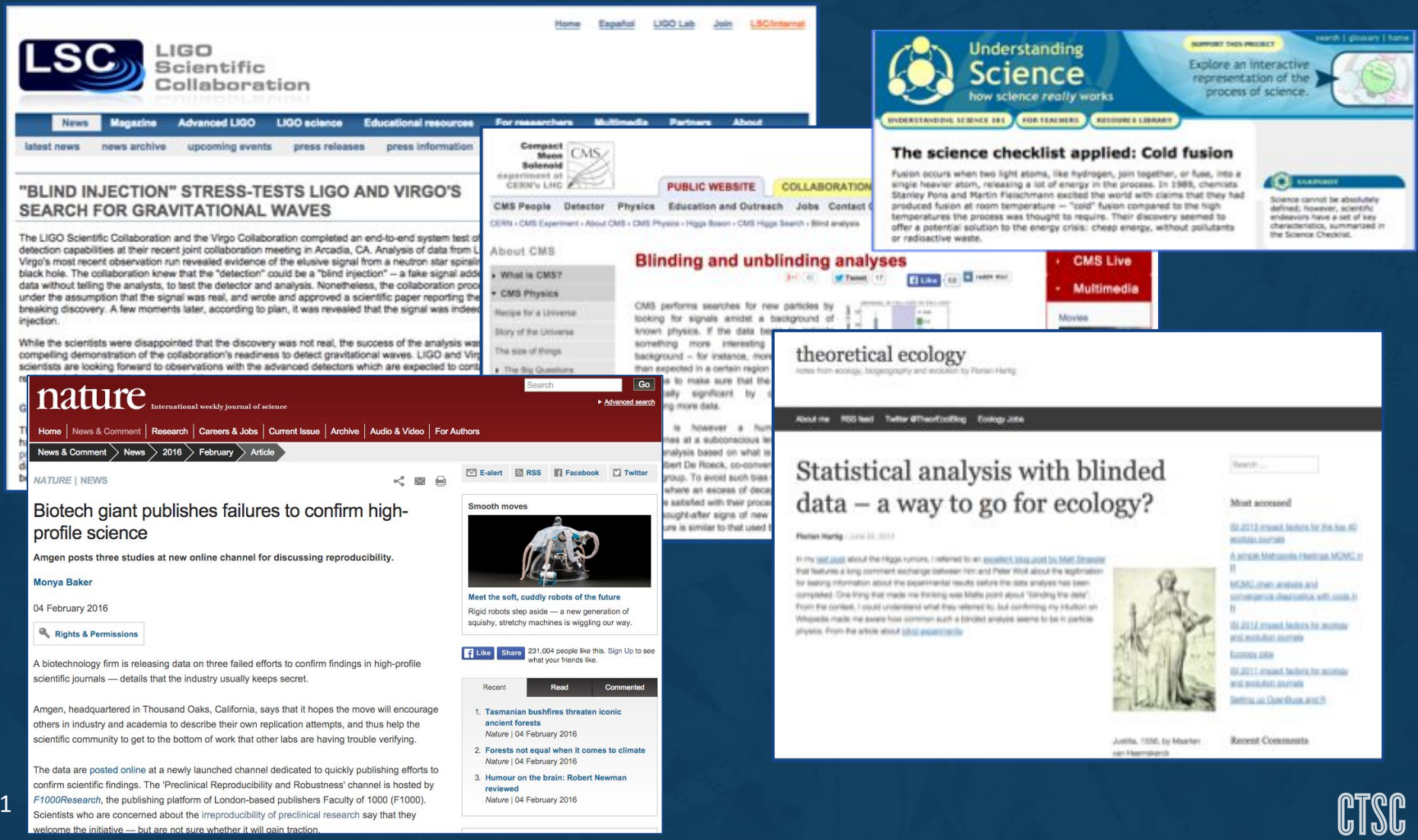
2. If we throw out a term that you don't understand, please stop us!

-2-
Cybersecurity & Science

Our information technology world is stormy



Science must be trustworthy and reproducible



CTSC

“But I don’t handle sensitive data….”

- Security is more than than confidentiality; the integrity and availability of data and instruments is critical for science.
- Confidentiality before “going public” with big news.
- Valuable data and powerful IT.
- Everyone is a target… “internet noise”; ransomware; and open science is… open!
- Threats? More than criminals and rivals… environmental risks; lax management.

“Isn’t this just an IT problem?”

Sadly, you cannot plug in and switch on a “solution” for information security.

Information security is about policy, procedures, technology, and people… and if you’re lucky, laws and regulations, too!

Policies provide the framework; procedures and technology can help implement the policy, but it really comes down to the people to understand/implement the concepts.

Information Security has a positive impact on the science even for smaller projects -- *it promotes best practices for IT!*

-3-
Cybersecurity Programs

So, what is a cybersecurity "program?"

A cybersecurity program is a structured approach to develop, implement, and maintain an environment conducive to appropriate levels of information security and risk to the organization's mission [i.e., your science mission].

Cybersecurity programs are made up of ongoing activities and projects in the areas of: policies and procedures; controls and mitigations; control verification and assessment; threat monitoring and activity analysis; incident response and remediation; and training and awareness.

Cybersecurity programs should be scoped to the key assets, resources, and lifespan of organizations.

Bottom line:

Security programs are living, breathing things.

CTSC

What does a PI or Project Manager want out of the cybersecurity program?

Enhance the science productivity by:

- Ensuring the availability of key information systems and processes that are critical to the science mission
- Guaranteeing the integrity of the data from accidental or malicious modification
- Protecting the confidentiality of private or sensitive information from accidental or malicious disclosure
- Obtaining these results while minimizing inconveniences and cost of the program

For more information …

trustedci.org/guide

and see also:

trustedci.org/ctsc-email-lists

trustedci.org/webinars

trustedci.org/useful-links

trustedci.org/trainingmaterials

Advantages of Cybersecurity From Day 0

- Least expensive, most effective.
- Make security a consideration of equipment, software, and service purchases.
- Get data storage/transport right so that you don't have to worry about trying to find/inventory later and wonder what was missed, mishandled, or stored outside project control.
- Avoid disturbing scientists' workflows in the course of retrofitting security measures after tech is in place.

-4-
Programmatic Must-Do's

Must-Do's

1. Classify and inventory data and information flows
2. Identify stakeholders
3. Identify roles and responsibilities
4. Develop core policies / procedures
5. Plan for and determine ownership of:
    a. Authentication and access controls
    b. Configuration and vulnerability management
    c. Monitoring (logs and network activity)
    d. Incident response and remediation
    e. Data recovery and retention
    f. Staff training and user awareness

1 Classification and Inventory

You can't secure what you can't identify and find.

A. Develop data classification scheme
   a. No more than 3-4 categories (public, private, sensitive)
   b. Define rules for data location and protection level
B. Identify critical systems; work with owners
   a. Data flows help identify critical information systems
   b. Based on criticality to project and compliance req'ts
   c. Availability and integrity are also important issues
C. Inventory the assets
   a. List assets and categorize by type and level of protection
   b. Develop in consultation with system owners
   c. Helps with cybersecurity resource allocation

2 Identify Stakeholders

- Project leadership. Involvement is essential.
- Institutions. Have requirements or provide resources
- Data subjects / research participants. Obligations?
- Funding agency. Involvement? Resources?

3 Identify Roles & Responsibilities

- Project leadership. Budget and set priorities for security, accept risk on behalf of the project, ultimately responsible for security.
- System owners. Understand capabilities/implications of systems and their interactions, advise project leadership and implement technical controls.
- Users / personnel. Understand how cybersecurity protects the science mission, practice good security hygiene.

4 Policies and Procedures

A little bit of planning can go a long way.

Developing some core policy results in:

- Getting people on the same page, *literally* (including stakeholders, new personnel, students)
- Enriched knowledge about your environment

Master Information Security Policy and Procedures (MISPP)

Purpose: Core, general policies + guide for navigating the full corpus of policies and procedures.

Audience: You and all your stakeholders.

- Roles & Responsibilities (... CISO, Leadership)
- Developing, Implementing, and Maintaining Our Cybersecurity Program (... core processes)
- Resources & Key Contacts (... we're here to help)
- Other Policy and Procedure Documents (... a gateway of sorts)
- Enforcement provisions
- Terms & Acronyms
- *… plus anything else so central to the program that it warrants stating here*

5 Plan for and determine ownership of ongoing operational activities

- Authentication and access controls
- Configuration and vulnerability management
- Monitoring (logs and network activity)
- Incident response and remediation
- Data recovery and retention
- Staff training and user awareness

Understand resources available to you at: https://protect.iu.edu/

http://researchtech.iu.edu/

Review existing program: https://protect.iu.edu/online-safety/program/safeguards/

Questions

Authentication and Authorization

Also referred to as Identity and Access Management (IAM)

Controls access to software and data - who is able to create, read, write, update, or delete

Includes processes for on-boarding and off-boarding

Configuration and Vulnerability Management

Default configurations are normally very insecure

Need to use accepted frameworks for secure initial configurations -- see Security Technical Implementation Guides (STIG); ensure configuration changes are approved and documented

Vulnerabilities in configuration or software arise on a continual basis -- need to do more than just scan; prioritize remediation

Monitoring

Compromises and intrusion WILL happen

Actively monitoring network traffic and logs can provide early detection

Pay close attention to outbound traffic to unexpected destinations

Incident Response and Remediation

Must have plans in advance for dealing with incidents; practice with table-top exercise

Having a good communication plan is important

Don’t be afraid to ask for help -- including institution, peers and law enforcement

Analyze for root cause of failure and repair

Data Recovery and Retention

Backups are essential to limit impact of data loss

Periodic testing data recovery process is essential for it to work when needed

Data retention policies and procedures can limit exposure in legal discovery cases

Staff Training and User Awareness

Everyone must be aware of key policies

Staff must understand procedures and processes and implement them

Users should be aware of the most recent forms of attack

Periodic training is necessary to remind and update

CTSC

CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

Thank You

trustedci.org

@TrustedCI

We thank the National Science Foundation (grant 1547272) for supporting our work.